Procedure No. 2205.14: Virtual Private Network (VPN) and Remote Access Policy
Reference: Policy No. 2205
Effective Date: 12/28/04
Prior Issue: n/a

Purpose

The Arizona Dept of Juvenile Corrections (ADJC) provides mandatory guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to ADJC network.

Rules:

1. **APPROVED AGENCY EMPLOYEES AND AUTHORIZED THIRD PARTIES (CUSTOMERS, VENDORS, CONTRACTORS, CONSULTANTS, TEMPORARIES, ETC.)** may utilize the benefits of VPNs, which are a "user managed" service. The **USER** is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

2. These **USERS** shall ensure that unauthorized users are not allowed access to ADJC’s internal networks.

3. These **USERS** shall follow these guidelines:
   a. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong pass phrase;
   b. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped;.
   c. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
   d. VPN gateways shall be set up and managed by ADJC network employees;
   e. All computers connected to ADJC internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard this includes personal computers;
   f. VPN users shall be automatically disconnected from ADJC's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open;
   g. The VPN connection is limited to an absolute connection time of 24 hours;
   h. Users of computers that are not Agency owned equipment must configure the equipment to comply with Agency's VPN and Network policies;
   i. Only ADJC approved VPN clients may be used;
   j. By using VPN technology with personal equipment, users shall understand that their machines are a de facto extension of ADJC 's network, and as such are subject to the same rules and regulations that apply to ADJC-owned equipment, i.e., their machines shall be configured to comply with ADJC's Security Policies while connect to the ADJC network.

4. **AGENCIES** may collectively establish inter-agency service agreements (ISAs) to implement and maintain a “trusted peer” relationship through encryption standards among multiple participants. **EACH PARTICIPANT IN THE AGREEMENT** shall agree to conform to all applicable requirements set forth in the agreement to ensure sufficient and acceptable security protection for all other participating agencies.

5. **ADJC EMPLOYEES, CONTRACTORS, VENDORS AND AGENTS WITH REMOTE ACCESS PRIVILEGES TO ADJC'S CORPORATE NETWORK** shall ensure that their remote access connection is given the same consideration as the user's on-site connection at ADJC.
   a. All information accessed remotely shall be held with the same confidentiality levels as the user’s on-site connection at ADJC;
   b. General access to the Internet for recreational use by immediate household members through the ADJC Network on personal computers is not permitted for employees.

c. Additional information regarding ADJC's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., is obtained by contacting MIS.
d. Secure remote access shall be strictly controlled in the highest sense. Control will be enforced via password authentication or public/private keys with strong pass-phrases.
e. At no time should any ADJC employee provide their login or email password to anyone, not even family members.
f. Routers for dedicated ISDN lines configured for access to the ADJC network must meet minimum authentication requirements of CHAP.
g. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
h. Frame Relay must meet minimum authentication requirements of DLCI standards.
i. Non-standard hardware configurations must be approved by Remote Access Services, and MIS must approve security configurations for access to hardware.
j. All hosts that are connected to ADJC internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers. Third party connections shall comply with these requirements.
k. Personal equipment that is used to connect to ADJC's networks shall meet minimum requirements of the remote management software.

6. **ADJC EMPLOYEES AND CONTRACTORS WITH REMOTE ACCESS PRIVILEGES** shall ensure that their agency owned or personal computer or workstation, which is remotely connected to ADJC's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

7. **ADJC EMPLOYEES AND CONTRACTORS WITH REMOTE ACCESS PRIVILEGES TO ADJC'S CORPORATE NETWORK** shall not use non-ADJC email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct ADJC business, thereby ensuring that official business is never confused with personal business.

8. **ORGANIZATIONS OR INDIVIDUALS** who wish to implement non-standard Remote Access solutions to the ADJC production network shall obtain prior approval from Remote Access Services and MIS.

9. **MIS** shall make available software for Agency, contracted or inter-agency employees to connect to ADJC resources for information securely.
a. **MIS** working with Intra-agency departments shall setup Interagency Service Agreements providing services for employees who need resources outside of ADJC's network securely.
i. Inter-agency service agreement form;
b. **MIS** shall continue to develop solutions for telecommuters, contractors, or off site employees to enhance productivity and work securely and safely;
c. **ADJC** Employees shall request for telecommuting access to be approved by their Supervisor and abide by all Human Resource policies governing telecommuting.
a. Remote Access Form Request

Effective Date:	Approved by Process Owner:	Review Date:	Reviewed By: